PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04L 9/00, 9/32

A1

(11) International Publication Number: **WO 00/64093**

(43) International Publication Date: 26 October 2000 (26.10.00)

(21) International Application Number: PCT/KR99/00713

(22) International Filing Date: 26 November 1999 (26.11.99)

(30) Priority Data:

1999/13820	19 April 1999 (19.04.99)	KR
1999/29376	20 July 1999 (20.07.99)	KR
1999/36341	30 August 1999 (30.08.99)	KR

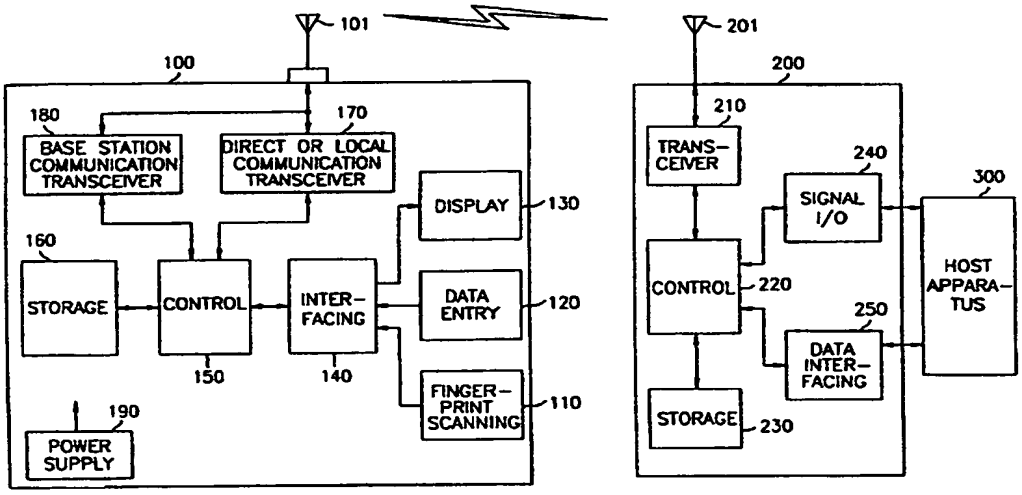
(71)(72) Applicant and Inventor: YOON, Tae, Sik [KR/KR]; 8–10th floor, Kyusudang B/D, 371–10, Seokyoe–dong, Mapo–Gu, Seoul 121–210 (KR).

(74) Agent: JANG, Seong, Ku; 17th floor, KEC Building, 275–7, Yangjae–dong, Seocho–ku, Seoul 137–130 (KR).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: WIRELESS PORTABLE DEVICE CAPABLE OF PERFORMING VARIOUS FUNCTIONS WITH ENHANCED SECURITY



(57) Abstract

A wireless communication system includes a multi–functional portable device and more than one host systems so as to accomplish various functions. The portable device performs at least one specific function with a host system and the host system has a transceiver and a host apparatus. Specifically, in order to achieve the purposes, the portable device includes a storage unit for storing at least a portion of information required in performing the specific function and a transceiver unit for transmitting the information to the host system in a form of an encrypted signal. The transceiver includes a control unit for decrypting the encrypted signal to reconstruct the information and a data interfacing unit for providing the reconstructed information to the host apparatus.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

WIRELESS PORTABLE DEVICE CAPABLE OF PERFORMING VARIOUS FUNCTIONS WITH ENHANCED SECURITY

TECHNICAL FIELD OF THE INVENTION

The present invention relates to a wireless portable communications system; and, more particularly, to a wireless portable device capable of performing such various functions as purchasing goods, payment, banking transaction or the like with an improved security.

BACKGROUND ART

Nowadays, as wireless communications techniques develop, wireless portable or mobile terminals such as cellular telephones have been widely used and it has also become possible to accomplish a data transmission as well as a voice signal transmission therethrough. Moreover, the use of the wireless portable terminals are gradually being extended to various applications in the art such as an internet, banking transactions and the like.

In addition to the extended use of the wireless portable terminals, machine-readable identification cards, such as credit cards, debit cards, point of sale (POS) cards, prepaid cards, automatic teller machine (ATM) cards, pass cards and the like, have become prevalent in such applications as performing credit sales transactions, payment of fees and gaining access to a restricted area.

For instance, in commercial banking, unattended banking terminals such as ATMs permit certain transactions. These transactions include accepting deposits, dispensing cash, transferring funds from one account to another, and making payments on credit card, utility or other accounts, or on mortgage or installment loans and the like. The customer is

required to present an identification card, which is often formed of a plastic medium and contains machine-readable information therein. This information includes, but is not limited to, the customer's account number, the identification number of the bank or institution, expiration date, credit limit, account balance and types of transactions authorized. The information is preferably contained in the card in the form of invisible magnetically recorded indicia, or could be contained in embossed indicia, apertures, or electrically conducting segments.

Further, the customer can perform those banking transactions with a telephone, a computer system, or the like without using any card. In this case, the customer has to input identification information of the customer through, e.g., the telephone, in order to initiate authorized banking transactions.

Therefore, for the above two cases of the unattended and the tele-banking transactions, when determining whether or not the customer is an authorized holder of the identification card presented at the banking terminal or an authorized tele-banking customer, secret data, such as a password or an identification number, along with account number and other transaction information are transmitted to a host or central banking computer over a communication line. However, by monitoring the communication line, it is possible for an unauthorized person to pick up the secret data of a customer and, with possession of the identification card, effect unauthorized transactions. Also, there is a disadvantage for the customer to have to remember the secret data.

Therefore, to overcome the above drawbacks, there are needs to enhance the security in the above and other transactions and further to make the customer easily perform the transactions without remembering the secret data while taking advantage of the convenience

of the wireless portable terminals.

DISCLOSURE OF THE INVENTION

It is, therefore, one object of the present invention to provide a multi-functional portable device for performing various functions in conjunction with more than one different host systems so as to take advantage of the convenience of portable devices and improve its transaction security.

Another object of the present invention is to provide a transceiver, incorporated with a host system, for effectively enabling a function to be carried out between the host system and the multi-functional portable device.

Still another object of the present invention is to provide a wireless communication system including a multi-functional portable device and more than one host systems each of which has a transceiver and a host apparatus in order to accomplish various functions therethrough and enhance its transaction security.

In accordance with one aspect of the present invention, there is provided a multi-functional portable device for performing various functions in conjunction with more than one different host systems, the portable device performing at least one specific function with a host system and communication between the portable device and the host system being carried out by wireless signals, comprising:

a storage unit for storing at least a portion of information required in performing said at least one specific function; and

a transceiver unit for transmitting the information to the host system in a form of an encrypted signal.

In accordance with another aspect of the present invention, there is provided a transceiver,

incorporated with a host apparatus, for enabling a function to be carried out between the host apparatus and a multi-functional portable terminal, the portable terminal transmitting an encrypted signal representing information required in performing the function, comprising:

a control unit for decrypting the encrypted signal to reconstruct the information; and

a data interfacing unit for providing the reconstructed information to the host apparatus.

In accordance with yet another aspect of the present invention, there is provided a wireless communication system including a multi-functional portable device and more than one host systems, wherein the portable device performs various functions in conjunction with the host systems, the portable device performing at least one specific function with a host system and the host system having a transceiver and a host apparatus, the portable device comprising:

a storage unit for storing at least a portion of information required in performing said at least one specific function; and

a transceiver unit for transmitting the information to the host system in a form of an encrypted signal, and

the transceiver comprising:

a control unit for decrypting the encrypted signal to reconstruct the information; and

a data interfacing unit for providing the reconstructed information to the host apparatus.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other objects and features of the present invention will become apparent from the following description of preferred embodiments given in conjunction with the accompanying drawings, in which:

Fig. 1 illustrates a schematic block diagram of a wireless communications system in accordance with the present invention;

Fig. 2 shows a first embodiment of the present invention;

Fig. 3 depicts a second embodiment of the present invention;

Fig. 4 describes a third embodiment of the present invention;

Fig. 5 provides a fourth embodiment of the present invention;

Fig. 6 represents a fifth embodiment of the present invention;

Fig. 7 shows a sixth embodiment of the present invention; and

Fig. 8 presents a seventh embodiment of the present invention.

MODES OF CARRYING OUT THE INVENTION

Referring to Fig. 1, there is provided a schematic block diagram of a wireless communications system for performing various functions. The system comprises a portable terminal 100, a transceiver 200 and a host apparatus 300. The host apparatus 300 can be an automatic engine starter, an actuator, an ATM, a host banking computer, a transport card terminal, a vending machine, a value-added network (VAN) terminal or the like, which will be illustrated hereinbelow.

In Fig. 1, the portable terminal 100 includes an antenna 101, a fingerprint scanning unit 110, a data entry unit 120, a display unit 130, an interfacing unit 140, a control unit 150, a storage unit 160, a direct or local communication transceiver unit 170, a base station communication transceiver unit 180 and a power supply unit 190.

The fingerprint scanning unit 110 scans a

fingerprint of a user and converts the scanned fingerprint image to electrical signals.

By using the data entry unit 120, the user can input data required in performing a selected function at the portable terminal 100.

The display unit 130 shows message data representing the processing status and information required to be reported to the user during the performance of the selected function.

The interfacing unit 140, connected between the control unit 150 and the fingerprint scanning, data entry and display units 110, 120 and 130, transmits signals or data, required in performing the selected function, between the units connected thereto, e.g., units 110, 120, 130 and 150.

The control unit 150 generally controls the operations of other components of the portable terminal 100. Specifically, if fingerprint data in the form of electrical signals are provided thereto via the interfacing unit 140 from the fingerprint scanning unit 110, the control unit 150 compares the fingerprint data with registered fingerprint data stored in the storage unit 160 to verify whether or not the user is an authorized user.

If the user is verified as a result of the comparison, the control unit 150 encodes or encrypts transaction information to output the encrypted information to the local communication transceiver unit 170 or the base station communication transceiver unit 180 depending on applications, as will be described with reference to Figs. 2 to 8. The transaction information may include transaction data representing the contents of the transaction to be carried out, personal identification data which includes, but is not limited to, a card number, an account number, a name of the user, password or a combination thereof, the fingerprint data, current time data or a combination

thereof according to a function to be performed.

In the present invention, the transaction information includes one of the fingerprint data of the user and the registered fingerprint data. In the preferred embodiment of the invention, the transaction information contains the registered fingerprint data stored in the storage unit 160.

If the authorized user operates the key pads of the data entry unit 120, numeral signals corresponding to the operated key pads or preset data corresponding to the operated key pads may be also encrypted and included in the above transaction information.

Herein, the current time data represent year, month, hour, minute and second. In case of a code division multiple access(CDMA) cellular phone, the current time is set by receiving time synchronous data provided by a base station. The current times of the base stations are synchronized under the control of a satellite.

In a preferred embodiment of the present invention, the fingerprint data can be representative feature data of the fingerprint of the user in order to reduce the volume of the data.

The storage unit 160 stores, but not limited to, the registered fingerprint data, basic personal identification data which may include, but are not limited to, e.g., a card number, an account number, password or the like needed for performing each function, a cryptographic algorithm, various communication programs and so on, and can be of a non-volatile memory, e.g., a flash memory, or preferably of a volatile memory having a power retention capability. In case a volatile memory is employed as the storage unit 160, the volatile memory is preferably associated with a subsidiary power storage device capable of maintaining the stored data in the storage unit 160 for a prolonged period when the power supply unit 190 is

discharged or unloaded. For security, the volatile memory is further provided with an associated device for erasing the data or information stored therein against the attempts of dissembling the portable terminal 100 or breaking into the memory system to take out the stored data, thereby preventing the stored data from being revealed to an unauthorized user when the portable terminal 100 is lost or stolen.

To transmit the encrypted information, the control unit 150 selects either the direct or local communication transceiver unit 170 or the base station communication transceiver unit 180 according to a function chosen among the functions that can be accomplished through a local area communication or a long-distance communication.

To perform the local area communication with the transceiver 200, the direct or local communication transceiver unit 170 modulates the encrypted information delivered from the control unit 150 to, e.g., radio frequency(RF) signals and transmits the modulated signals via the antenna 101 to the transceiver 200. Furthermore, optionally, during the performance of the selected function, the direct communication transceiver unit 170 may receive signals from the transceiver 200 and demodulate the received signals so as to provide the demodulated signals to the control unit 150.

On the other hand, in order to accomplish the long-distance communication with the transceiver 200, there needs a base station(not shown) to relay the transmission signals between the portable terminal 100 and the transceiver 200. The base station communication transceiver unit 180 converts the encrypted information transferred from the control unit 150 to, e.g., CDMA signals; modulates the converted signals into, e.g., RF signals; and transmits the modulated signals via the antenna 101 to a base

station(not shown). In addition, during the performance of the selected function, the base station communication transceiver unit 180 may receive signals from the transceiver 200 via the base station and demodulate the received signals to thereby provide the demodulated signals to the control unit 150.

The control unit 150 can choose either the direct or local communication transceiver unit 170 or the base station communication transceiver unit 180 according to the characteristic of the selected function to be performed by the portable terminal 100. That is, if the selected function is adapted to the local area communication, the direct or local communication transceiver unit 170 is chosen and, if otherwise, the base station communication transceiver unit 180 is selected.

The power supply unit 190 provides a DC voltage to each component of the portable terminal 100 and is preferably a rechargeable battery.

Meanwhile, as illustrated in Fig. 1, the transceiver 200 comprises an antenna 201, a transceiver unit 210, a control unit 220, a storage unit 230, a signal input/output(I/O) unit 240 and a data interfacing unit 250.

The transceiver unit 210 receives the transmission signals delivered from the direct communication transceiver unit 170 or the base station communication transceiver unit 180 of the portable terminal 100 via the communication channel; demodulates the received signals; and transfers the demodulated signals to the control unit 220. Moreover, optionally, during the performance of the selected function, the transceiver unit 210 can modulate signals or information provided from the control unit 220 and transmit the modulated signals or information via the antenna 201 to the portable terminal 100.

The control unit 220 decrypts the demodulated

signals provided from the transceiver unit 210 by using a cryptographic algorithm stored in the storage unit 230 to thereby provide control or display signals corresponding to the decrypted signals to a host apparatus 300 via the signal I/O unit 240 while outputting functional data derived from the demodulated signals to the host apparatus 300 via the data interfacing unit 250.

In a preferred embodiment of the present invention, a time gate scheme is employed to enhance the security. In that case, the control unit 220 compares the time data included in the decrypted signals with a time data representing the current time in the transceiver 200. As a result of the comparison, only if the time difference determined by the time data transmitted from the portable terminal 100 and that of the transceiver 200 is within a predetermined range, e.g., a data propagation time from the transceiver unit 170 or 180 to the control unit 220, the transmitted data from the portable terminal 100 is determined as the valid data. In other words, only if the difference is equal to or smaller than a predetermined threshold value, the control or display signals, or the functional data is transferred to the host apparatus 300 via the signal I/O unit 240 or the data interfacing unit 250.

In accordance with another preferred embodiment of the invention, verification of data in accordance with the inventive time gate scheme is performed by the host apparatus 300 in lieu of the transceiver 200. In that case, the decrypted signals are transferred to the host apparatus 300 without being subject to the verification of data, which is then carried out at the host apparatus 300.

In accordance with the time gate scheme of the invention, the current times of the portable terminal 100 and the transceiver 200(or the host apparatus 300)

are periodically synchronized and, therefore, are set to be identical all the time. Further, the current time at an instance when the portable terminal 100 encodes or encrypts the transaction information is included therein and then compared with the current time at an instance when the transceiver 200 or the host apparatus 300 receives the transaction information. Accordingly, the security of the transaction is highly preserved since an unauthorized user cannot reuse the transmission signals obtained accidently or intentionally from the communication channel or network unless he or she decrypts the whole transmission signals and makes up new transmission signals by replacing the current time data. The inventive time gate scheme can provide enhanced security but is simple and easy to implement because time synchronization of the system can be achieved by existing communication networks, e.g., CDMA PCS(personal communications services) networks, without having to employ additional complicated time synchronization schemes as in the prior art and time data itself is directly compared with the current time of the receiving end without using rather complex time-based codes.

In a preferred embodiment, the current time at the portable terminal 100 and the current time at the transceiver 200(or the host apparatus 300) can be synchronized by time synchronization data provided by base stations or a satellite in, e.g., existing CDMA communication networks. Therefore, as can be seen above, the inventive time gate scheme can be employed in the preferred embodiments if desired by way of incorporating a device into either the transceiver 200 or the host apparatus 300 capable of receiving the time synchronization data.

Referring back to Fig. 1, the associated operations of the portable terminal 100 and the

transceiver 200 will be more specifically explained hereinafter.

Prior to all of operations, a user first sets the portable terminal 100 to a fingerprint registration mode by manipulating the data entry unit 120 and registers his/her fingerprint data, produced by scanning the user's fingerprint through the use of the fingerprint scanning unit 110, in the storage unit 160 to accomplish the fingerprint registration process. The fingerprint data are encrypted and then stored in order to avoid being revealed to unauthorized users when the portable terminal 100 is lost or stolen.

Some of the functions which can be provided by the portable terminal 100 may not need the fingerprint authentication depending on the levels of security they require, as will be described with reference to the embodiments of Figs. 2 to 8. For instance, if a transaction or a function does not involve a large amount of money and the security level required is not critical, the fingerprint authentication process can be omitted for the sake of convenience. For the purpose of illustration, however, it is assumed that the fingerprint authentication process is required and the process is generally described hereinbelow.

After completing the fingerprint registration process, if a user places a finger on the fingerprint scanning unit 110 by which a fingerprint of the finger is scanned, fingerprint feature data corresponding to the user's finger are generated and then provided to the control unit 150 via the interfacing unit 140.

Upon receiving the fingerprint data provided thereto, the control unit 150 compares the fingerprint data with the registered fingerprint data previously stored in the storage unit 160 so as to determine whether the user is an authorized user or not.

If the result of the comparison is negative, i.e., if the user is determined as not to be the authorized

user, the control unit 150 terminates the fingerprint authentication process and instructs the display unit 130 to display thereon a message representing the failure of the fingerprint authentication.

On the other hand, if the result of the comparison is positive, i.e., if the user is determined as the authorized user, the control unit 150 encrypts transaction information including the fingerprint data, the current time data of the portable terminal 100, the transaction data representing the content of a function to be carried out and required in performing the function, the personal identification data which may include a card number, an account number, password or the like required in performing the function, or a combination thereof by using the cryptographic algorithm stored in the storage unit 160. The control unit 150 then outputs the encrypted information to the direct or local communication transceiver unit 170 or the base station communication transceiver unit 180 while displaying a message showing that the function or the transaction is under process on the display unit 130.

In the preferred embodiment of the invention, the personal identification data for each function are all prestored in the storage unit 160 and, therefore, need not be inputted by the user on a function basis. The transaction data may also be generated automatically without requiring a user's input. In some applications, however, at least some of the transaction data may need to be inputted by the user. For instance, if a function being performed is of a tele-banking, the user may have to make a selection among services provided or have to input a transaction account. In such a case, the control unit 150 prompts the user to input data by delivering the requisite message on the display unit 130.

At this time, if the user provides some data

within a preset time after being prompted by manipulating the data entry unit 120, information corresponding to the input data is also encrypted and included in the transaction information by the control unit 150; and the encrypted information is provided to the direct or local communication transceiver unit 170 or the base station communication transceiver unit 180. Herein, if there is no input data from the data entry unit 120 within the preset time after being urged, the function or the transaction is terminated.

The processing order of the above operations can be changed in accordance with the embodiments of the present invention. That is, the data entry operation can be performed prior to the fingerprint authentication.

In a case of the local area communication, data transmission between the portable terminal 100 and the transceiver 200 may be carried out by the infrared ray signals. In that case, the antenna 101 would be to be of the type implemented by a photo diode and a photo detector.

The transceiver unit 210 receives the modulated signals transmitted through the communication channel from the portable terminal 100; demodulates the received signals; and transfers the demodulated signals to the control unit 220. Herein, when the signals are transmitted in the form of the infrared ray signals, the antenna 201 is also of the type implemented by a photo diode and a photo detector.

The control unit 220 decrypts the demodulated signals provided from the transceiver unit 210 through the use of the cryptographic algorithm stored in the storage unit 230; constructs the original information corresponding to the encrypted information outputted from the portable terminal 100 based on the decrypted signals; and provides the reproduced information to the host apparatus 300 via the signal I/O unit 240 or the

data interfacing unit 250 according to the characteristics of the reproduced information.

In accordance with another preferred embodiment of the invention, prior to delivering the reproduced information to the host apparatus 300, the inventive time gate scheme and/or the fingerprint authentication process can be performed at the transceiver 200. In that case, the time gate scheme is accomplished as described above in detail and the fingerprint authentication process is carried out by the control unit 220 in the same manner as in the portable terminal 100 based on the fingerprint data included in the reproduced information and the fingerprint data prestored in the storage unit 230. In this case, registration of the fingerprint data in the storage unit 230 can be accomplished by using an external fingerprint scanning apparatus which can be connected to the transceiver 200.

Hereinafter, referring to Figs. 2 to 8, there are illustrated exemplary embodiments of the present invention, which will be explained in conjunction with Fig. 1.

Referring to Fig. 2, there is illustrated a first exemplary embodiment of the present invention applied in remote-starting of an automobile. The inventive transceiver 200 is connected to an automatic engine starter 400.

The automatic engine starter 400 can be of a kind being used in conventional remote-controlled vehicle engine starting systems. In such a case, the portable terminal 100 acts as a remote control transmitter for providing an engine start signal; the transceiver 200, a receiver for capturing and feeding the transmitted engine start signal to the automatic engine starter 400; and the automatic engine starter 400, an engine starting circuit for starting the engine in response to the transmitted engine start signal.

In this embodiment, if the automatic vehicle starting function is selected, e.g., by inputting a corresponding code via the data entry unit 120 so that the portable terminal 100 is initiated to perform the selected vehicle starting function, fingerprint data of a user of the portable terminal 100 are provided through the fingerprint scanning unit 110 and provided to the control unit 150 via the interfacing unit 140. Upon successful fingerprint authentication, the control unit 150 retrieves from the storage unit 160 and encrypts a vehicle starting signal containing the fingerprint data. The encrypted signal is modulated at the direct communication transceiver unit 170 and then transmitted to the transceiver 200 through the communication channel, i.e., the air. This embodiment assigns about 300 bytes to the transmission of the vehicle starting signal.

Once the transceiver 200 receives the modulated signal, the control unit 220 compares the fingerprint data detected from the received signal with registered fingerprint data stored in the storage unit 230. If the result of the comparison is positive, i.e., the fingerprint authentication is accomplished, a control signal is provided to the automatic engine starter 400. Then, the automatic engine starter 400 automatically starts the engine of the vehicle in response to the control signal. Also, the automatic engine starter 400 may include appropriate circuits for automatically operating various accessory electrical equipment in the vehicle such as the headlights, heater, air conditioner, defroster, etc. Since the operation of the automatic engine starter 400 is similar to that of an engine starting circuit of a conventional remote-controlled vehicle engine starting system, the explanation thereof will not be repeated for the sake of simplicity.

In this embodiment, the fingerprint data need be

prestored in the storage unit 230. In that case, registration of the fingerprint data can be accomplished prior to installing the transceiver 200 in the automobile by using an external fingerprint scanning apparatus which can be connected to the transceiver 200. The security level required in this embodiment may not be so critical, and, therefore, the time gate scheme of the invention may not be employed in this embodiment. The time gate scheme, however, can be employed in this embodiment if desired by way of incorporating a device into the transceiver 200 capable of receiving the time synchronization data from a base station.

In another embodiment of the present invention applied in the remote-starting of the automobile, the fingerprint authentication process may be performed only at the portable terminal 100. In that case, the storage unit 230 does not need store the registered fingerprint data therein and fingerprint data need not be included in the vehicle starting signal transmitted from the portable terminal 100.

Although the above embodiment has been described with reference to the automatic vehicle engine starting function, it is to be understood that the present invention can be applied to any machinery which requires the automatic starting operation.

Now, referring to Fig. 3, there is illustrated a second exemplary embodiment of the present invention applied in a remote-controlled door lock system which remotely unlocks or locks an automatic door. Herein, the transceiver 200 is connected to an actuator 500.

The actuator 500 can be also of a kind being used in conventional remote-controlled door lock systems. In such a case, the portable terminal 100 simply acts as a remote control transmitter for providing a door lock control signal; the transceiver 200, a receiver for capturing and feeding the transmitted door lock

control signal to the actuator 500; and the actuator 500, a door lock circuit for locking or unlocking the automatic door in response to the transmitted door lock control signal.

The operation of the present invention related to the remote-controlled door lock system is similar to that of the first embodiment. That is, if the remote-controlled door lock function is selected, e.g., by inputting a corresponding code via the data entry unit 120, the portable terminal 100 is initiated to perform the selected door lock function. Thereafter, a door lock control signal containing fingerprint data of a user are transferred to the transceiver 200 through the communication channel, i.e., the air, only if the fingerprint authentication is successfully accomplished.

Once the transceiver 200 receives the door lock control signal transmitted from the portable terminal 100, the control unit 220 detects the fingerprint data of the user from the received door lock control signal and compares them with registered fingerprint data prestored in the storage unit 230. If the result of the comparison is positive, i.e., the fingerprint authentication is accomplished, a control signal is provided to the actuator 500. Then, the actuator 500 automatically locks or unlocks the automatic door in response to the control signal.

In this embodiment, the fingerprint authentication at the transceiver 200 may not be employed as in the first exemplary embodiment. Further, the time gate scheme may be or may not be employed as in the first exemplary embodiment.

Referring to Fig. 4, there is illustrated a third exemplary embodiment of the present invention applied in ATM systems, wherein the portable terminal 100 performs an ATM card function and is used in lieu of a machine-readable identification card such as a credit

card or an ATM card. In this embodiment, the transceiver 200 is connected to an ATM 600 and a predetermined portion of the storage unit 160 is assigned to store data or information, such as a card number, password, etc., required to perform the ATM card function.

Specifically, if the ATM card function is selected, e.g., by inputting a corresponding code via the data entry unit 120, the portable terminal 100 is initiated to perform the selected ATM card function. Then, upon the successful fingerprint authentication, the portable terminal 100 transmits transaction information through the direct communication transceiver unit 170 to the transceiver 200 connected to or embodied in the ATM 600, wherein the transaction information includes, but is not limited to, a corresponding card number and password, which are stored in the storage unit 160.

Once the transaction information is fed to the transceiver 200, the control unit 220 decrypts the transmitted transaction information and, then, the decrypted transaction information is transferred to the ATM 600 without being subject to the verification of data, which is carried out at the ATM 600 based on the decrypted transaction information as in the prior art. If the access to the ATM 600 is permitted through the data verification at the ATM 600, the user can accomplish the desired banking transactions by operating the ATM 600 in the same manner as in the prior art using the machine-readable identification cards. The transactional operations at the ATM 600 is not germane to the subject invention and, therefore, the details thereof will not be described for the sake of simplicity.

In another preferred embodiment of the present invention applied to the ATM system, the fingerprint authentication is employed. In that case, after the

successful fingerprint authentication, the portable terminal 100 provides the transceiver 200 with transaction information which further includes the fingerprint data of the verified user.

Once the transaction information is fed to the transceiver 200, the control unit 220 decrypts the transmitted transaction information including the fingerprint data and provides the decrypted transaction information via the ATM 600 to a host banking computer(not shown) connected to the ATM 600. In this case, the host banking computer carries out the verification of the transaction information by further comparing the fingerprint data included in the transaction information with registered fingerprint data recorded in authorized user files in the host banking computer through the fingerprint authentication process depicted above. As a result, if the user is verified as an authorized user, the desired banking transactions are performed in the same manner as in the prior art.

In further another preferred embodiment, the present invention can employ the time gate scheme for enhancing the security of the banking transactions instead of or together with the fingerprint authentication. In that case, the time gate scheme may be performed by way of the transceiver 200, the ATM 600 and the host banking computer if they are provided with devices for capturing the time synchronization data so that the time thereat is synchronized with that at the portable terminal 100. However, it may be most preferably that the time comparison is carried out at the host banking computer.

Referring to Fig. 5, there is illustrated a fourth exemplary embodiment of the present invention applied to a phone banking. The transceiver 200 is connected to or embodied in a host banking computer 700 and a predetermined portion of the storage unit 160 of the

portable terminal 100 is assigned to store data or information required to perform the phone banking.

For the phone banking, the security of the banking transactions is of vital importance since an unauthorized user may be able to obtain access to user identification information by electronic eavesdropping, reducing the security provided by this banking system. Therefore, this embodiment utilizes the time gate scheme described above together with the fingerprint authentication to improve its security.

In accordance with this embodiment, if a user chooses the phone banking function to thereby set up the call connection to the host banking computer 700 and initiate the phone banking function by way of, e.g., inputting a corresponding code number or calling the host banking computer 700 and the portable terminal 100 determinates the user to be an authorized one as a result of the fingerprint authentication process, transaction information, including, but not limited to, the personal identification data having a user's identification number, an account number, password, etc., the user's fingerprint data and the time data representing a current time at the portable terminal 100, are encrypted and modulated at the portable terminal 100. The modulated signals are then transmitted via a base station 750 to the transceiver 200 connected, e.g., between a host banking computer 700 and the base station 750.

Once the modulated signals are inputted to the transceiver 200, the control unit 220 demodulates and decrypts the received signals to restore the original transaction information and transfers the decrypted transaction information to the host banking computer 700.

If the decrypted transaction information is coupled thereto, the host banking computer 700 performs the data verification, the fingerprint authentication

and the time gate processes as described in the third embodiment.

If the current user is determined as an authorized user as the results of the data verification, the fingerprint authentication and the time gate processes, requested transactions can be accomplished between the portable terminal 100 and the host banking computer 700 by transceiving required information therebetween as in the prior art.

Referring to Fig. 6, there is illustrated a fifth exemplary embodiment of the present invention incorporating transport, e.g., bus and/or subway, card functions in the portable terminal 100, which can be used to pay transport fares instead of conventional transport cards. For this embodiment, a predetermined portion of the storage unit 160 is assigned to store data or information required to perform the transport card functions and the data transmission of the portable terminal 100 is accomplished via the direct communicating transceiver unit 170 since the portable terminal 100 for this embodiment is operable only when it is placed close to a transport card terminal 800.

In this embodiment, when the portable terminal 100 is placed within a predetermined distance from the transport card terminal 800, the portable terminal 100 is automatically initiated to perform the transport card function, e.g., by receiving an establishing signal which is continuously broadcasted from the transceiver 200.

For instance, in case the portable terminal 100 is used instead of a bus card which is of a prepaid card, a prepaid amount of money is recorded in a predetermined portion of the storage unit 160 in the portable terminal 100. After then, when the portable terminal 100 is positioned within the predetermined distance from the transport card terminal 800, the portable terminal 100 is automatically set to perform

the bus card function and a bus fare is transferred together with portable terminal information from the portable terminal 100 to the transport card terminal 800 via the direct communicating transceiver unit 170 and the transceiver 200. The prepaid amount of money is then updated by deducting the bus fare therefrom.

In case the portable terminal 100 contains a subway card function therein, the portable terminal 100 is automatically set to perform the subway card function by receiving the establishing signal broadcasted from the transceiver 200 when the portable terminal 100 is placed within the predetermined distance from the transport card terminal 800. And then, since the subway card function is generally combined to a credit card, credit card information previously stored in a predetermined portion of the storage unit 160 of the portable terminal 100 is extracted and transmitted to the transceiver 200.

If the encrypted credit card information is transferred thereto, the transceiver 200 decrypts the encrypted credit card information and provides the decrypted information to the transport card terminal 800 through the data interfacing unit 250. Then, the transport card terminal 800 performs the remaining processes to accomplish the subway card function as in the prior art.

In order to enhance the security, the transport card function can be performed after authenticating fingerprint data of a user at the portable terminal 100. That is, before transmitting the portable terminal information or the credit card information, the fingerprint data of the user are inputted to the portable terminal 100 through the fingerprint scanning unit 110 and the portable terminal 100 performs the fingerprint authentication by comparing the inputted fingerprint data with the registered fingerprint data stored in the storage unit 160. After the fingerprint

authentication is successfully accomplished, the required information, i.e., the portable terminal information or the credit card information, can be transmitted from the portable terminal 100 to the transport card terminal 800.

Referring to Fig. 7, there is illustrated a sixth exemplary embodiment of the present invention incorporating a prepaid card, a debit card or a credit card function, an electronic money or a combination thereof in the portable terminal 100 to purchase a desired product from a vending machine 900. Similarly to the above illustrated embodiments, a predetermined portion of the storage unit 160 is assigned to store data or information required to implement this embodiment.

In this embodiment, if this function is selected, e.g., by inputting a corresponding code via the data entry unit 120 so that the portable terminal 100 is initiated to perform the selected function, a user inputs a preset amount of money to be needed to use the vending machine 900 by using the data entry unit 120 and chooses a payment method among the various card function and the electronic money. After the above processes are performed, the control unit 150 encrypts and modulates the preset amount of money together with payment information corresponding to the chosen payment method, e.g., card information, and then transmits the modulated information to the transceiver 200 connected to or embodied in the vending machine 900.

The transceiver 200 demodulates and decrypts the received information to provide the decrypted information to the vending machine 900 via the data interfacing unit 250 so that the user can obtain products corresponding to the preset amount of money from the vending machine 900.

In accordance with another embodiment of this function, in order to enhance the security, the

fingerprint authentication process is performed at the portable terminal 100 before transmitting the modulated information. As a result, if the fingerprint authentication is successfully accomplished, the modulated information can be transmitted to the transport card terminal 800.

Referring to Fig. 8, the present invention can be associated with a VAN terminal 950 to pay a fare or a price of a product by using the portable terminal 100 having a credit card function therein. This embodiment also has a predetermined portion of the storage unit 160 assigned to store data or information required to implement the credit card function.

First of all, if this credit card function is selected, e.g., by inputting a corresponding code via the data entry unit 120, the portable terminal 100 is initiated to perform the selected credit card function. After then, if a price to be paid is inputted to the VAN terminal 1100, the price is transferred to the portable terminal 100 via the transceiver 200 and displayed on the display unit 130 of the portable terminal 100. Then, if a user sequentially provides installment information and fingerprint data to the portable terminal 100 through the data entry unit 120 and the fingerprint scanning unit 110, respectively, the installment information and the fingerprint data are encrypted together with card information retrieved from the storage unit 160 and then transmitted to the transceiver 200 via the direct communication transceiver unit 170.

The transceiver 200 decrypts the encrypted information transmitted from the portable terminal 100 and delivers the decrypted information to the VAN terminal 950 through the data interfacing unit 250.

The VAN terminal 950 transfers the installment information, the price of the product, the card information and the fingerprint data to a VAN

company(not shown) in order to get a transactional permission. In accordance with this embodiment, the VAN company performs a transaction authentication based on the fingerprint data and the card information in order to determine whether or not permitting the required transaction.

If the transaction is permitted and a permission number therefor is received from the VAN company, the VAN terminal 950 transfers the permission number to the transceiver 200, which then encrypts the permission number and transmits it to the portable terminal 100. The portable terminal 100 receives the transmitted permission number and displays it on the display unit 130. Through the processes, the transaction is completed.

In accordance with another embodiment, the fingerprint data may be used for the user authentication only at the portable terminal 100 without being transmitted to the transceiver 200.

If the portable terminal 100 incorporates therein an electronic money function, it is possible to transfer money between two portable terminals situated nearby. For instance, if a user of a portable terminal wants to send a predetermined amount of money to a use of another portable terminal, the user of the first portable terminal selects the electronic money transfer function by inputting a corresponding code and then inputs a predetermined amount of money to be transferred and an identification information verifying the second portable terminal, e.g., a telephone number. Thereafter, the user of the first portable terminal provides his or her fingerprint data through the fingerprint scanning unit 110 for fingerprint authentication. After the authentication is successfully accomplished and the first portable terminal is connected to the second portable terminal, the first portable terminal transmits an instruction

signal to the second portable terminal through the direct communication transceiver unit 170. The second portable terminal prepares a money transmission protocol in response to the instruction signal and sends a ready signal representing that the second terminal is ready to accept the money to be transferred. Once the first portable terminal receives the ready signal from the second portable terminal to thereby recognize that the protocol is prepared, the first portable terminal sends transfer data representing the predetermined amount of money being transferred to the second portable terminal. Upon receiving the transferred data, the second portable terminal issues a transfer completion signal indicating a safe receipt of the transferred money at the second portable terminal and stores a sum of the amount of money transferred and the previous amount of money stored in a storage thereof. Meanwhile, the first portable terminal receives the transfer completion signal from the second portable terminal and stores therein an amount of money determined by subtracting the amount of money transferred from the previous amount of money stored in a storage thereof if the successful money transfer is verified between the first portable terminal and the second portable terminal. It is to be understood that the electronic money transfer described above can be achieved between two portable terminals spaced apart via a base station.

It is to be understood that the portable terminal 100 can selectively employ one of the direct communication transceiver unit 170 and the base station communication transceiver unit 180. If only the direct communication transceiver unit 170 is employed in the portable terminal 100, the portable terminal 100 can perform functions associated with local area communications only. On the other hand, if only the base station communication transceiver unit 180 is

employed in the portable terminal 100, all the functions described above can be accomplished via a base station.

In a preferred embodiment of the invention, the aforementioned functions are preferably implemented by using a wireless portable phone, e.g., a PCS phone, a cellular phone or the like, further employing the direct communication transceiver unit 170 and the fingerprint scanning unit 110 therein. However, a terminal, which employs the direct communication transceiver unit 170 and optionally incorporates the fingerprint scanning unit 110, can also accomplish the above functions other than the phone banking requiring the long-distance communication. Therefore, it will be apparent to those skilled in the art that the portable terminal 100 can be of a type other than a wireless portable phone.

In the preferred embodiment of the invention, the signals or data transmitted between the transceiver 200 and a conventional host apparatus, e.g., an automatic vehicle starting apparatus, an ATM, a transport card terminal, a VAN terminal, or the like, are preferably of the types identical to those of the signals or data between the host apparatus and conventional input/output terminals thereof; and the transceiver 200 is coupled to the conventional host apparatus in parallel with the conventional input/output terminals thereof. In this way, the inventive transceiver 200 can be easily incorporated with the conventional host apparatus. That is, by using the transceiver 200 generating the signals or data identical to those for the conventional apparatus, it is possible to perform a related function between the above inventive wireless portable terminal and the conventional host apparatus without altering the configuration thereof.

In order to select specific functions to be performed by the portable terminal 100, two selection

schemes are employed as described above: one is that a user selects a specific function by inputting a selection code corresponding to the specific function through the data entry unit 120; and the other is that the transceiver 200 specified to the host system performing the specific function continuously broadcasts an establishing signal in a predetermined narrow area close thereto and, then, the portable terminal 100 receives the establishing signal to thereby perform the specific function in response to the establishing signal. Even though each function has been described as being activated by only one of the two schemes in the present invention, it is to be understood that the portable terminal 100 can be devised to initiate each function by the other one of the schemes or by both the schemes.

In another embodiment of the present invention, biometric data other than the fingerprint data can be used for the user's authentication.

While the present invention has been described with respect to the particular embodiments, it will be apparent to those skilled in the art that various changes and modifications may be made without departing from the spirit and scope of the invention as defined in the following claims.

What is claimed is:

1. A multi-functional portable device for performing various functions in conjunction with more than one different host systems, the portable device performing at least one specific function with a host system and communication between the portable device and the host system being carried out by wireless signals, comprising:

a storage unit for storing at least a portion of information required in performing said at least one specific function; and

a transceiver unit for transmitting the information to the host system in a form of an encrypted signal.

2. The multi-functional portable device as recited in claim 1 further comprising:

means for selecting said at least one specific function.

3. The multi-functional portable device as recited in claim 2, wherein the selecting means is a data entry unit.

4. The multi-functional portable device as recited in claim 2, wherein the host system has means for generating an establishing signal and the selecting means chooses said at least one specific function in response to the establishing signal.

5. The multi-functional portable device as recited in claim 2 further comprising:

a fingerprint scanning unit for providing a fingerprint data of a user.

6. The multi-functional portable device as recited in

claim 5, wherein a registered fingerprint data is prestored in the storage unit.

7. The multi-functional portable device as recited in claim 6, wherein the encrypted signal is sent to the host system only if the registered fingerprint data and the fingerprint data of the user are determined to be identical.

8. The multi-functional portable device as recited in claim 7, wherein the information includes one of the registered fingerprint data and the fingerprint data of the user.

9. The multi-functional portable device as recited in claim 8, wherein the host system has fingerprint data and said at least one specific function is accomplished only if the fingerprint data included in the encrypted signal is determined to be identical to the fingerprint data in the host system.

10. The multi-functional portable device as recited in claim 7, wherein a time at the portable device is synchronized with that at the host system and the information includes time data representing a time at which the portable device generates the encrypted signal.

11. The multi-functional portable device as recited in claim 10, wherein said at least one specific function is accomplished only if the time represented by the time data and a time at which the host system receives the encrypted signal is within a predetermined range.

12. The multi-functional portable device as recited in claim 8, wherein a time at the portable device is synchronized with that at the host system and the

information includes time data representing a time at which the portable device generates the encrypted signal.

13. The multi-functional portable device as recited in claim 12, wherein the host system has fingerprint data and said at least one specific function is accomplished only if the fingerprint data included in the encrypted signal is determined to be identical to the fingerprint data in the host system and the time represented by the time data and a time at which the host system receives the encrypted signal is within a predetermined range.

14. The multi-functional portable device as recited in claim 7, wherein the transceiver unit is for a local area communication and the portable device communicates with the host system directly.

15. The multi-functional portable device as recited in claim 7, wherein the portable device is a wireless phone and the transceiver unit is for a long-distance communication and wherein the portable device communicates with the host system via a base station.

16. The multi-functional portable device as recited in claim 14 further comprising a transceiver device for a long-distance communication, wherein the portable device is a wireless phone and communicates with the host system directly through the use of the transceiver unit or communicates with the host system via a base station through the use of the transceiver device.

17. A transceiver, incorporated with a host apparatus, for enabling a function to be carried out between the host apparatus and a multi-functional portable terminal, the portable terminal transmitting an encrypted signal representing information required in

performing the function, comprising:

a control unit for decrypting the encrypted signal to reconstruct the information; and

a data interfacing unit for providing the reconstructed information to the host apparatus.

18. The transceiver according to claim 17 further comprising:

means for generating an establishing signal, wherein the function is selected at the portable terminal in response to the establishing signal.

19. A wireless communication system including a multi-functional portable device and more than one host systems, wherein the portable device performs various functions in conjunction with the host systems, the portable device performing at least one specific function with a host system and the host system having a transceiver and a host apparatus, the portable device comprising:

a storage unit for storing at least a portion of information required in performing said at least one specific function; and

a transceiver unit for transmitting the information to the host system in a form of an encrypted signal, and

the transceiver comprising:

a control unit for decrypting the encrypted signal to reconstruct the information; and

a data interfacing unit for providing the reconstructed information to the host apparatus.

20. The wireless communication system as recited in claim 19, wherein the portable device further comprising:

means for selecting said at least one specific function.

FIG. 1

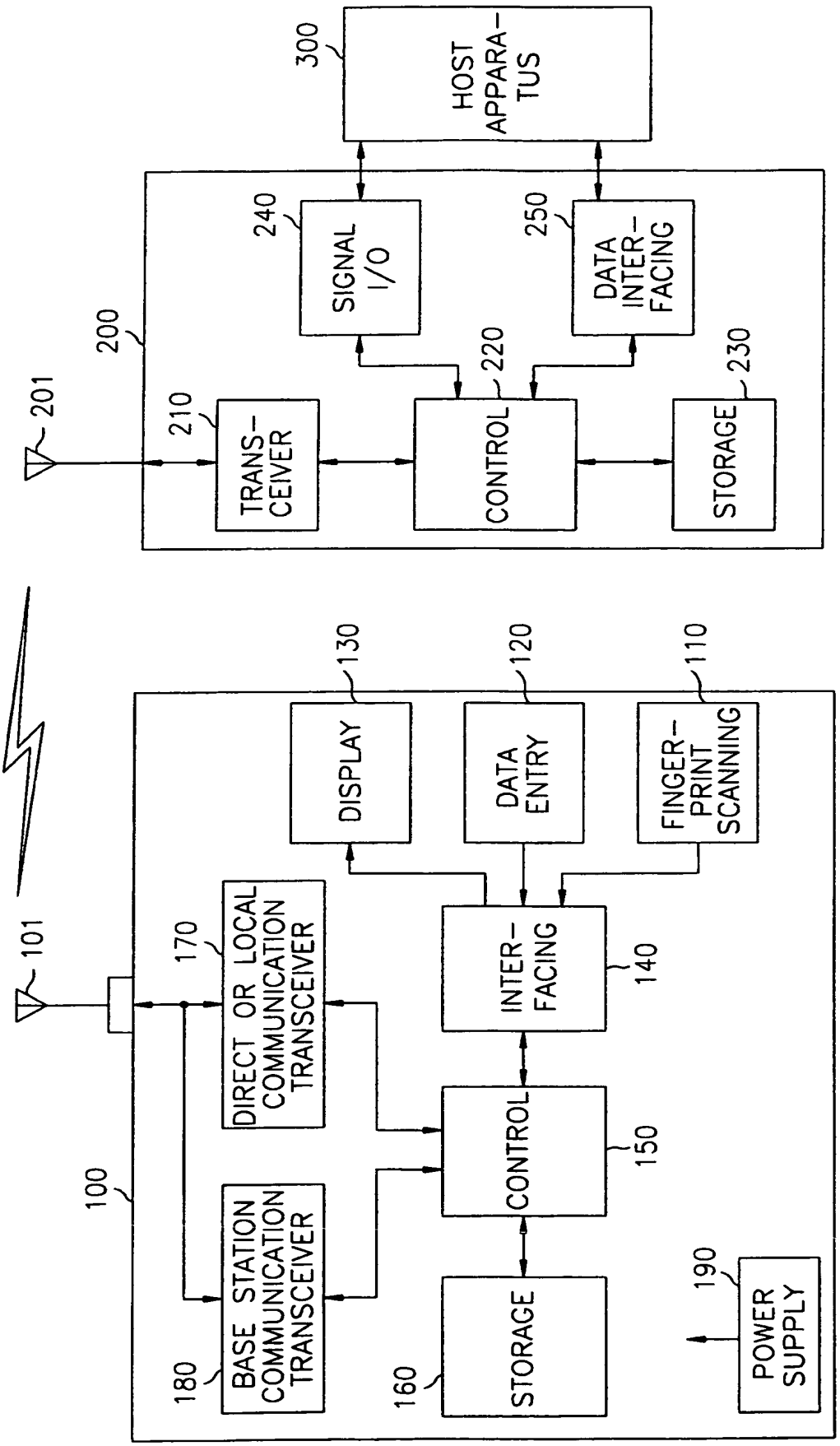

300
HOST APPARA-TUS
240
SIGNAL I/O
250
DATA INTER-FACING
200
201
210
TRANS-CEIVER
220
CONTROL
230
STORAGE
130
DISPLAY
120
DATA ENTRY
110
FINGER-PRINT SCANNING
101
170
DIRECT OR LOCAL COMMUNICATION TRANSCEIVER
INTER-FACING
140
100
CONTROL
150
BASE STATION COMMUNICATION TRANSCEIVER
180
160
STORAGE
190
POWER SUPPLY

FIG.2

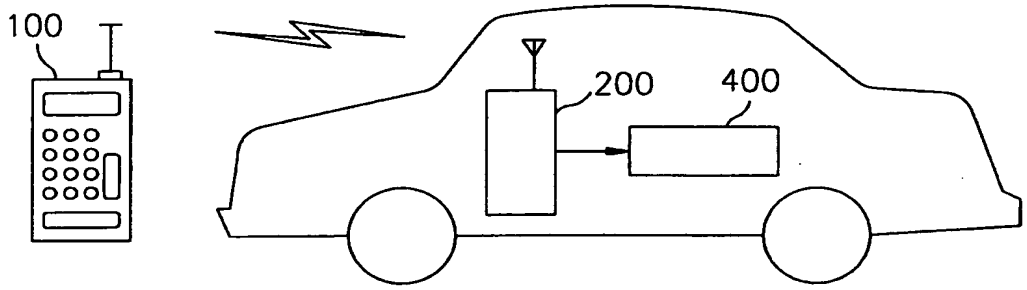


FIG.3

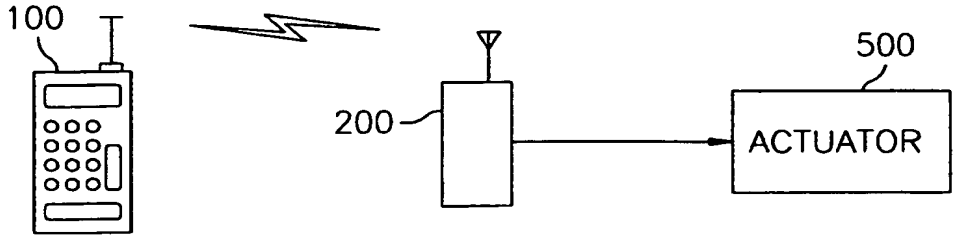


FIG.4

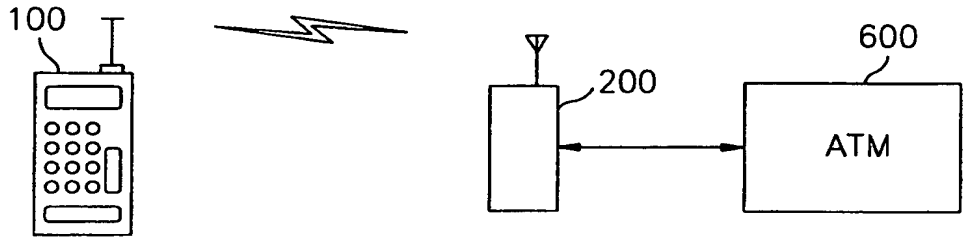


FIG.5

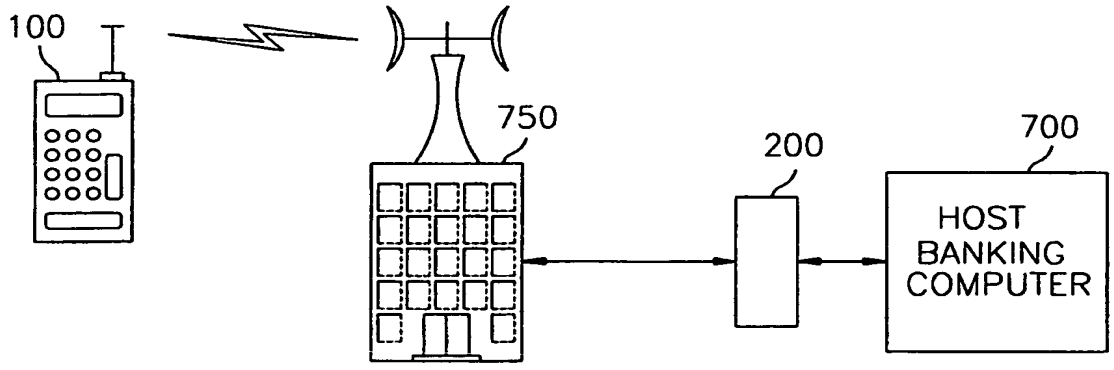


FIG.6

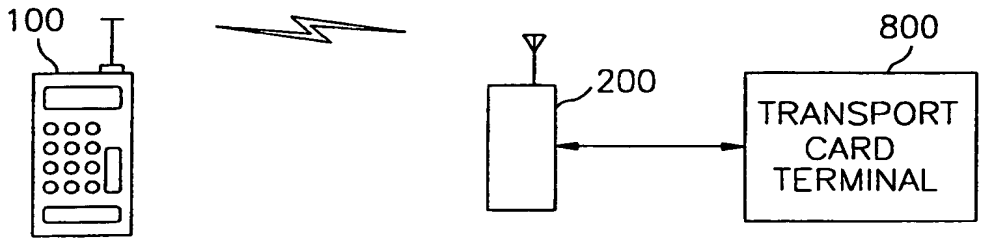

100
200
800
TRANSPORT CARD TERMINAL

FIG.7

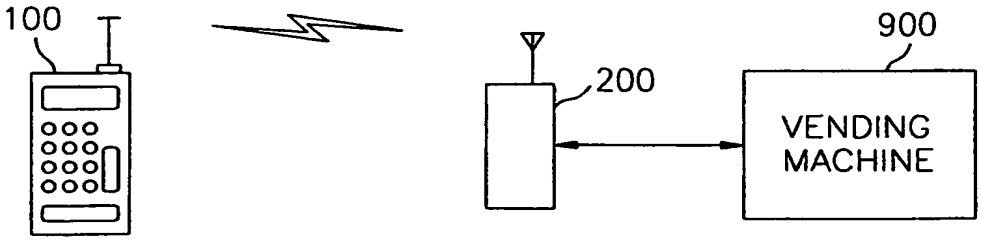
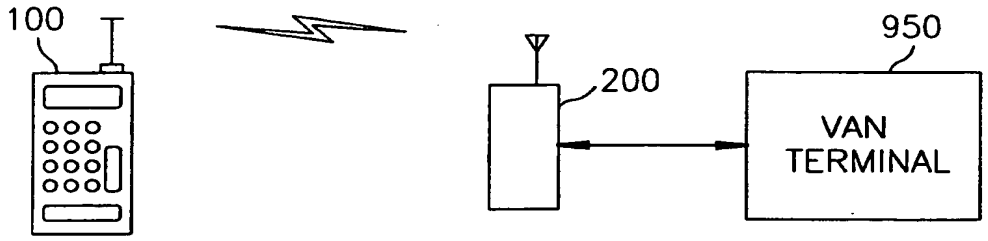

100
200
900
VENDING MACHINE

FIG.8



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR 99/00713

CLASSIFICATION OF SUBJECT MATTER

IPC[7]: H 04 L 9/00, 9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC[7]: H 04 L 5/00, 9/00, 9/28, 9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

H 04 B 7/00, 7/24, 7/26; G 06 K 17/00

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5203017 A (BROOKS) 13 April 1993 (13.04.93)	1,17,19
A	EP 0670556 A1 (GEMPLUS) 6 September 1995 (06.09.95)	1

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
„A" document defining the general state of the art which is not considered to be of particular relevance
„E" earlier application or patent but published on or after the international filing date
„L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
„O" document referring to an oral disclosure, use, exhibition or other means
„P" document published prior to the international filing date but later than the priority date claimed

„T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
„X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
„Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 April 2000 (27.04.2000)	31 July 2000 (31.07.2000)
Name and mailing adress of the ISA/AT Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/535	Authorized officer Grössing Telephone No. 1/53424/386

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR 99/00713

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
US	A	5203017	13-04-1993	US	A	5220677	15-06-1993
EP	A1	670556	06-09-1995	FR	A1	2716988	08-09-1995
				FR	B1	2716988	26-04-1996
				JP	A2	7271888	20-10-1995
				US	A	5635701	03-06-1997

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR 99/00713

Both documents retrieved exhibit a multi-functional portable communication device capable of payments or banking via wireless signals and including storage facilities. The US 5203017 A also includes a transceiver unit for transmitting information to the host.